



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,770	08/27/2003	Ram Gopal Lakshmi Narayanan	27592-00454-US	4039
30678 7590 08/07/2009 CONNOLLY BOVE LODGE & HUTZ LLP 1875 EYE STREET, N.W. SUITE 1100 WASHINGTON, DC 20006				
EXAMINER				
DINH, MINH				
ART UNIT		PAPER NUMBER		
2432				
MAIL DATE		DELIVERY MODE		
08/07/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary**Application No.**

10/648,770

Applicant(s)NARAYANAN, RAM GOPAL
LAKSHMI**Examiner**

MINH DINH

Art Unit

2432

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 April 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 6-16, 33-41, 45 and 46 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 6-16, 33-41, 45 and 46 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 August 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Response to Amendment

1. This office action is in response to the amendment filed on 04/09/09. Claims 1-2, 4, 7-8, 11, 13, 16, 33-36 and 38-41 are amended.

Response to Arguments

2. Applicant's arguments filed 04/09/09 have been fully considered but they are not persuasive. Applicant argues that the digital signature generated by the receiving end DS2 would have to match one generated by the sending end DS1 as explained in the attached paper from SearchSecurity.com (Remarks, page 9). The attached paper clearly discloses that the receiver decrypts the signature (i.e., encrypted hash) generated by the sender with the sender's public key rather than generating another signature using the sender's public key as disclosed in the specification.
3. Applicant's arguments filed 04/09/09 have been fully considered but they are not persuasive. Applicant argues that Moy does not teach or suggest: (i) monitoring a specific multicast channel of a plurality of multicast channels, the specific multicast channel, being for sending jump-start messages by a node to other nodes when the node has not received any messages from said other nodes on said specific multicast channel; (ii) sending a jump-start message on said specific multicast channel from a start node that has not received any messages on said specific multicast channel, wherein the jump-start message is secured by the start node and the start node starts an operation or an application; and (iii) upon receiving the jump-start message at a

receiving node an authenticity of the jump-start message is validated (Remarks, page 10, last paragraph).

First, Moy discloses that a node monitors a specific multicast channel (i.e., AllSPRouters multicast address) for hello packets from its neighbors in order to determine whether the neighbors are active, the hello packet being functionally equivalent to a jump-start message (Section 9.5 – Sending Hello packets).

Second, Moy discloses that the node keeps sending hello packets to its neighbor even though it has not received hello responses for a period of time (Section 10.3 - The neighbor state machine; Section C.3 – Router interface parameters: HelloInterval, RouterDeadInterval).

Third, Moy discloses verifying the authenticity of OSFP packet by a receiving node, the hello packet being an OSFP packet (Section A.3.2 – The Hello packet; Section D.5.3 – Verifying Cryptographic authentication).

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1-16, 35, 40 and 45 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use

the invention. Regarding claim 1, it recites the limitation "an authenticity of the jump-start message is validated" The specification discloses that the start node R1 generates a digital signature DS1 for the jump-start message by encrypting the source address and a random value using the private key of R1, i.e., $DS1 = \text{Enc}(\text{Source Address}, \text{Random Value}, \text{Private Key of Router 1})$ (paragraphs 0040-0045). The specification then discloses that the receiving node R2 receives the jump-start message together with signature DS1 and validates the authenticity of the jump-start message by: generating a digital signature DS2 by encrypting the source address and the random value retrieved from the start message using the public key of R1, i.e., $DS2 = \text{Enc}(\text{Source Address}, \text{Random Value}, \text{Public Key of Router 1})$; comparing DS1 and DS2, and determining that the start message is authentic if $DS1 = DS2$ (paragraphs 0046-0048). However, it is well known in cryptography art that the values of the public key and the private key of a public/private key pair are not supposed to be the same. As a result, the signatures DS1 and DS2 disclosed in the specification would never be the same when the private key and the public key used in the process are valid keys and that the start message is authentic. Thus, the disclosure fails to enable one skilled in the art to make and use the claimed invention. Claim 16 is rejected on the same basis as claim 1. Claims 35 and 40 also recite signing the jump-start message and, therefore, are rejected on the same basis as claim 1. Claims that are not specifically addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1, 3, 6, 33, 35, 37-38, 40 and 45-46 are rejected under 35 U.S.C. 102(b) as being anticipated by Moy ("RFC 2328 – OSPF Version 2"). Moy discloses a method performed in a communication system including a plurality of nodes, i.e., routers implemented in OSPF routing protocol, communicating in a shared network segment and at least one multicast channel in said shared network segment (Section 1, Introduction; figure 1a, Broadcast networks), the method comprising: monitoring a specific multicast channel (i.e., AllSPRouters multicast address) of a plurality of multicast channels, the specific multicast channel, being for sending jump-start messages by a node to other nodes when the node has not received any messages from said other nodes on said specific multicast channel (Section 9.5 – Sending Hello packets); sending a jump-start message on said specific multicast channel from a start node that has not received any messages on said specific multicast channel, wherein the jump-start message is secured by the start node and the start node starts an operation or an application (Section 10.3 - The neighbor state machine; Section C.3 – Router interface parameters: HelloInterval, RouterDeadInterval), wherein upon receiving the jump-start message at a receiving node an authenticity of the jump-start message is

validated (Section A.3.2 – The Hello packet; Section D.5.3 – Verifying Cryptographic authentication).

8. Claims 1, 3-4, 6, 33, 35, 37-38, 40 and 45-46 are rejected under 35

U.S.C. 102(b) as being anticipated by Murphy et al. ("Digital Signature Protection of the OSPF Routing Protocol") as evidenced by Moy ("RFC 2328 – OSPF Version 2").

Murphy discloses protection of routing information exchanged between routers in OSPF routing protocol using digital signature (Abstract). Specifically, Murphy discloses that when a sending router sends routing information message to a receiving router, the sending router signs the message using its private key so that the receiving router can verify the signature using the public key of the sending router to determine the authenticity of the message (Section 4, Using digital signature in OSPF). Murphy does not disclose sending a jump-start message on said specific multicast channel from a start node that has not received any messages from its neighbors on said specific multicast channel; however, Moy discloses that this feature is inherent to the OSPF routing protocol (Section 10.3 - The neighbor state machine; Section C.3 – Router interface parameters: HelloInterval, RouterDeadInterval).

9. Claims 1, 3-4, 6-8, 10-12 and 33, 35-38, 40-41 and 45-46 are rejected under 35 U.S.C. 102(b) as being anticipated by Nguyen et al. (2002/0016926) as evidence by Moy ("RFC 2328 – OSPF Version 2").

Regarding claims 1, 3-4, 6, 33, 35, 37-38, 40 and 45-46 Nguyen discloses a method and system for securely exchanging routing information among routers, i.e., secure gateway devices (SGDs), in OSPF routing protocol using encryption (Abstract;

paragraphs 0088, 0101). Specifically, Nguyen discloses that when a sending router sends routing information message to a receiving router, the sending router encrypts the message using an encryption key (paragraphs 0102, 0104-0105). Nguyen does not explicitly disclose sending a jump-start message on said specific multicast channel from a start node that has not received any messages from its neighbors on said specific multicast channel; however, Moy discloses that this feature is inherent to the OSPF routing protocol (Section 10.3 - The neighbor state machine; Section C.3 – Router interface parameters: HelloInterval, RouterDeadInterval).

Regarding claims 7-8, 10, 36 and 41, Nguyen does not explicitly disclose sending the multicast messages from the nodes comprising routers including a Designated Router and other routers; determining that the Designated Router comprises an only available node in a shared segment if the Designated Router does not receive a response or the start message from the other nodes when only the Designated Router comprises an active node in a shared network segment; however, Moy discloses that this feature is inherent to the OSPF routing protocol (Section 1.2, Definitions of Commonly Used Terms; Section 4.3, Routing protocol packets; Section 7.1, The Hello Protocol; Section 7.3, The Designated Router). Nguyen further discloses generating a session key for encrypting multicast routing information, e.g., routing updates, using ISAKMP (paragraphs 104-105, 110-111).

Regarding claims 11-12, Nguyen further discloses engaging in Internet Key Exchange (IKE) protocol between routers involved in a communication session to generate security associations (paragraphs 0024-0025, 0105, 0119). Nguyen also

discloses secure multicast communication among routers (paragraphs 0110-0111). Inherently, security associations used for unicast communication are different from those used for multicast communication.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 2, 34 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moy as applied to claims 1, 33 and 38. Moy does not disclose monitoring by the start node for a predefined time to determine whether messages are sent on the specific third multicast channel before sending the jump-start message from the start node. Official Notice is taken that both concept and advantage of monitoring a communication channel for a predefined period of time to determine whether messages are sent on the channel before sending a message using the channel to avoid contention and collision of data transmission are well known and expected in the art. It would have been obvious to have monitored by the start node for a predefined time to determine whether messages are sent on the specific third multicast channel before sending the jump-start message from the start node in Moy to avoid contention and collision of data transmission.

12. Claims 2, 34 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy as evidenced by Moy as applied to claims 1, 33 and 38. Murphy and Moy do not disclose monitoring by the start node for a predefined time to determine whether messages are sent on the specific third multicast channel before sending the jump-start message from the start node. Official Notice is taken that both concept and advantage of monitoring a communication channel for a predefined period of time to determine whether messages are sent on the channel before sending a message using the channel to avoid contention and collision of data transmission are well known and expected in the art. It would have been obvious to have monitored by the start node for a predefined time to determine whether messages are sent on the specific third multicast channel before sending the jump-start message from the start node in Murphy and Moy to avoid contention and collision of data transmission.

13. Claims 2, 34 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen as evidenced by Moy as applied to claims 1, 33 and 38. Nguyen and Moy do not disclose monitoring by the start node for a predefined time to determine whether messages are sent on the specific third multicast channel before sending the jump-start message from the start node. Official Notice is taken that both concept and advantage of monitoring a communication channel for a predefined period of time to determine whether messages are sent on the channel before sending a message using the channel to avoid contention and collision of data transmission are well known and expected in the art. It would have been obvious to have monitored by the start node for a predefined time to determine whether messages are sent on the specific third

multicast channel before sending the jump-start message from the start node in Nguyen and Moy to avoid contention and collision of data transmission.

14. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen as evidence by Moy as applied to claim 7, and further in view of Kaliski, Jr. (6,085,320). Nguyen, discloses using ISAKMP (Internet Security Association and Key Management Protocol) (paragraph 0105). Inherent to ISAKMP, each party in a two-party communication session generates a session key using a random number, its own private key and the other party's public key (according to Diffie-Hellman algorithm); however, a timestamp is not used to generate the session key in ISAKMP. Kaliski discloses using a timestamp (i.e., a time-varying value) in generating a session key (col. 5, lines 34-38). It would have been obvious to one of ordinary in the art at the time the invention was made to modify the Nguyen method to use a timestamp in generating the session key, as taught by Kaliski, in order to prevent replay attack.

15. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen as evidence by Moy as applied to claim 1 above, and further in view of Srivastava et al. (7,103,185). Nguyen discloses using security associations for unicast/multicast communication between routers (paragraphs 0104-0105, 0110). Nguyen does not explicitly disclose a Designated Router and a Backup Designated Router connected (i.e., adjacent) to each other and to other routers in the network; however, Moy discloses that this feature is inherent to the OSPF routing protocol (Section 7.3, The Designated Router; Section 7.4, The Backup Designated Router). Nguyen does not disclose changing the session key for a multicast group when a new

member joins the multicast group or when a member leaves the multicast group. Srivastava discloses a method for management of session keys in a multicast group comprising generating a new session key for a multicast group by a designated member when a new member joins the multicast group or when a member leaves the multicast group (col. 2, lines 58-67; figures 4B-C; col. 11, line 50 – col. 12, line 45). Srivastava also discloses generating a new session key for a multicast group when a member leaves the multicast group (col. 2, lines 58-67). It would have been obvious to one of ordinary in the art at the time the invention was made to modify the Nguyen method to change the session key for a multicast group when a new member joins the multicast group or when a member leaves the multicast group, as taught by Srivastava. The motivation for doing so would have been to prevent the new member from decrypting past messages and the member who leaves from deciphering future messages of the multicast group.

Allowable Subject Matter

16. Subject to the above 112, 1st paragraph rejections, claim 16 would be allowable over the prior art of record.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MINH DINH whose telephone number is (571)272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Minh Dinh/
Examiner, Art Unit 2432

08/03/09